

# **STEGANOGRAFI PADA CITRA DIGITAL MENGGUNAKAN METODE *SPREAD SPECTRUM* DAN METODE *LEAST SIGNIFICANT BIT (LSB) MODIFICATION***

## **TUGAS AKHIR**

Diajukan Sebagai Salah Satu Syarat  
Untuk Memperoleh Gelar Sarjana Teknik Pada  
Jurusan Teknik Informatika

oleh :

**BUDI PRANOTO**  
**10451025507**



FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU  
PEKANBARU  
2011

# **STEGANOGRAFI PADA CITRA DIGITAL MENGGUNAKAN METODE *SPREAD SPECTRUM* DAN METODE *LEAST SIGNIFICANT BIT (LSB) MODIFICATION***

**BUDI PRANOTO**

**NIM : 10451025507**

Tanggal Sidang : 27 Juni 2011  
Periode Wisuda : November 2011

Jurusan Teknik Informatika  
Fakultas Sains dan Teknologi  
Universitas Islam Negeri Sultan Syarif Kasim Riau  
Jl. Soebrantas No.155 Pekanbaru

## **ABSTRAK**

Seiring dengan berkembangnya media internet dan aplikasi yang menggunakan internet semakin bertambah pula kejahatan dalam sistem informasi. Salah satu cara dalam mengamankan data dan informasi adalah melalui teknik steganografi. Steganografi pada citra digital dapat dijadikan alternatif untuk menyimpan data rahasia ke dalam wadah citra digital. Steganografi dapat juga digunakan untuk menyampaikan pesan rahasia, karena sifat dari steganografi yang sulit dideteksi keberadaannya.

Pengembangan aplikasi steganografi pada citra digital dengan menggunakan metode *spread spectrum* dalam pengacakan pesan dan menggunakan metode *least significant bit modification* dalam penyembunyian pesan. *LSB* bekerja dengan menggantikan bit-bit terakhir pada berkas citra digital dengan bit data yang berupa data pesan yang akan disembunyikan.

Dari penelitian ini diperoleh hasil bahwa mutu berkas citra digital yang telah disisipi pesan tidak mengalami perubahan berarti dan data yang berada dalam citra digital dapat diekstraksi kembali. Namun berkas citra digital yang telah disisipi pesan tidak tahan terhadap proses editing (kompresi, pemotongan, perubahan ukuran, dan proses editing lainnya) yang dilakukan pada berkas citra digital tersebut.

Kata Kunci : Citra Digital, *Least-Significant Bit Modification*, *Spread Spectrum*, Steganografi,

***IMAGE STEGANOGRAPHY USING SPREAD SPECTRUM  
METHOD AND LEAST SIGNIFICANT BIT (LSB)  
MODIFICATION METHOD***

**BUDI PRANOTO**

**NIM : 10451025507**

*Hearing Date : June, 27<sup>th</sup> 2011  
Graduation Period : November 2011*

*Informatics Departement  
Faculty of Sciences and Technology  
State Islamic University of Sultan Syarif Kasim Riau  
Soebrantas Street No.155 Pekanbaru*

***ABSTRACT***

*Along with the development of Internet media and applications that use the internet more and also increased crime in the information system. One way of securing data and information is through the technique of steganography. Steganography in digital images can be used as an alternative to storing confidential data into a digital image of the container. Steganography can also be used to convey secret messages, due to the nature of steganography is difficult to detect its presence.*

*Steganography application development on digital image by using the method of spread spectrum in the randomization of messages and using the method of least significant bit modification, the concealment of this message to work by replacing the last bits on the digital image file with a bit of data in the form of data messages to be hidden.*

*From this study obtained results that the quality of digital image files that have been inserted the message unchanged and the data in digital image can be extracted again. However, the digital image file that has been inserted message is not resistant to the editing process (compression, cropping, resizing, and other editing processes) are performed on the digital image file.*

*Key Words: Digital Image, Least-Significant Bit Modification, Spread Spectrum, Steganography,*

## DAFTAR ISI

	Halaman
LEMBAR PERSETUJUAN.....	ii
LEMBAR PENGESAHAN .....	iii
LEMBARAN HAK ATAS KEKAYAAN INTELEKTUAL .....	iv
LEMBARAN PERNYATAAN .....	v
LEMBARAN PERSEMBAHAN .....	vi
ABSTRAK .....	vii
<i>ABSTRACT</i> .....	viii
KATA PENGANTAR .....	ix
DAFTAR ISI.....	xi
DAFTAR GAMBAR .....	xv
DAFTAR TABEL.....	xvii
DAFTAR ISTILAH .....	xviii
DAFTAR SIMBOL.....	xx
 BAB I PENDAHULUAN .....	 I-1
1.1 Latar Belakang.....	I-1
1.2 Rumusan Masalah.....	I-2
1.3 Batasan Masalah .....	I-2
1.4 Tujuan .....	I-2
1.5 Sistematika Penulisan .....	I-3
 BAB II LANDASAN TEORI .....	 II-1
2.1 Steganografi.....	II-1
2.1.1 Sejarah Steganografi .....	II-3
2.1.2 Manfaat Steganografi.....	II-4
2.1.3 Metode Steganografi.....	II-4

2.1.3.1 Modifikasi LSB .....	II-4
2.1.3.2 <i>Spread Spectrum</i> .....	II-7
2.2 Citra Digital .....	II-7
2.2.1 Konsep Dasar Citra Digital .....	II-8
2.2.2 Jenis Citra Digital.....	II-8
2.2.2.1. Citra biner ( <i>Monochrome</i> ) .....	II-9
2.2.2.2. Citra skala keabuan ( <i>grayscale</i> ).....	II-9
2.2.2.3. Citra warna ( <i>true color</i> ) .....	II-10
2.2.3 Citra Bitmap .....	II-10
 BAB III METODOLOGI PENELITIAN.....	III-1
3.1 Identifikasi Masalah .....	III-2
3.2 Penetapan tujuan .....	III-2
3.3 Pengumpulan Data.....	III-2
3.4 Analisa Sistem .....	III-2
3.5 Perancangan Sistem .....	III-3
3.6 Implementasi dan Pengujian.....	III-3
3.7 Kesimpulan dan Saran .....	III-4
 BAB IV ANALISA DAN PERANCANGAN .....	IV-1
4.1 Deskripsi Metode.....	IV-1
4.1.1 Deskripsi Metode Penyisipan Data Pesan Dengan <i>Spread spectrum</i> .....	IV-1
4.2 Analisa Perangkat Lunak .....	IV-4
4.2.1 Spesifikasi Sistem .....	IV-4
4.2.1.1 Kebutuhan Perangkat Lunak .....	IV-5
4.2.1.2 Tujuan Pengembangan Perangkat Lunak .....	IV-5
4.2.1.3. Arsitektur Perangkat Lunak .....	IV-5
4.2.2. Kebutuhan Fungsional .....	IV-6

4.3. Perancangan Perangkat Lunak .....	IV-6
4.3.1. Perancangan Flowchart .....	IV-8
4.3.1.1. Flowchart Penyisipan .....	IV-9
4.3.1.2. Flowchart Ekstraksi .....	IV-10
4.3.2 Perancangan Antarmuka Sistem .....	IV-11
4.3.2.1 Antarmuka Menu Utama .....	IV-11
4.3.2.2 Antarmuka input Password .....	IV-12
 BAB V IMPLEMENTASI DAN PENGUJIAN .....	V-1
5.1 Implementasi .....	V-1
5.1.1 Batasan Implementasi .....	V-1
5.1.2 Lingkungan Implementasi .....	V-1
5.1.2.1 Lingkungan Perangkat Keras .....	V-1
5.1.2.2 Lingkungan Perangkat Lunak .....	V-2
5.2 Pengujian .....	V-2
5.2.1 Pengujian Tampilan Aplikasi Steggambar .....	V-2
5.3 Deskripsi Pengujian .....	V-6
5.3.1 Pengujian Modul Menyembunyikan Teks Dalam berkas citra digital. ....	V-6
5.3.1.1 Pengujian Tahap I Mencari sumber Citra digital dan Lokasi penyimpanan .....	V-7
5.3.1.2 Pengujian Tahap 2 Memasukkan Data Pesan Yang Akan Disembunyikan .....	V-8
5.3.1.3 Pengujian Tahap 3 Proses Steganografi dan Memasukkan Kata Kunci .....	V-9
5.3.2 Pengujian Modul Mengambil Data Pesan Dalam Berkas Citra Digital .....	V-10
5.3.2.1 Pengujian Tahap 1 Menentukan Berkas Citra ..... Hasil Stegano Yang Akan Diambil Data Pesannya	V-10

5.3.2.2 Pengujian Tahap 2 Memasukkan Kata Kunci .....	V-11
5.3.2.3 Pengujian Tahap 3 Mengambil Data Pesan Teks ....	
Dalam Berkas Citra Digital .....	V-12
5.4. Pengujian Berdasarkan Kriteria Steganografi .....	V-13
5.4.1 Pengujian Berdasarkan <i>Imperceptibility</i> .....	V-13
5.4.2 Pengujian Berdasarkan <i>Fidelity</i> .....	V-14
5.4.3 Pengujian Berdasarkan <i>Recovery</i> .....	V-14
5.4.4 Pengujian Kesesuaian Data .....	V-15
5.4.5 Pengujian Berdasarkan Robustness .....	V-16
5.4.5.1 Pengujian Proses Editing 1: <i>Cropping</i> .....	V-16
5.4.5.2 Pengujian Proses Editing 2: <i>Rotate</i> .....	V-17
5.4.5.3 Pengujian Proses Editing 3: <i>Resize</i> .....	V-18
5.5 Kesimpulan Pengujian .....	V-20
 BAB VI PENUTUP .....	 VI-1
6.1 Kesimpulan .....	VI-1
6.2 Saran .....	VI-1
 DAFTAR PUSTAKA	
LAMPIRAN	
DAFTAR RIWAYAT HIDUP	

## DAFTAR TABEL

Tabel	Halaman
4.1 Keterangan antarmuka menu utama aplikasi Stegambar .....	IV-9
4.2 Keterangan antarmuka <i>input password</i> untuk menulis pesan pada gambar .....	IV-10
4.3 Keterangan antarmuka <i>input password</i> untuk membaca pesan pada gambar .....	IV-11
5.1 Butir uji pengujian tahap 1 mencari sumber citra digital dan lokasi penyimpanan .....	V-7
5.2 Butir uji pengujian tahap 2 memasukkan data pesan yang akan disembunyikan .....	V-8
5.3 Butir uji pengujian tahap 3 proses steganografi dan memasukkan kata kunci .....	V-9
5.4 Butir uji pengujian tahap 1 menentukan berkas citra digital hasil steganografi yang akan diambil data pesannya .....	V-10
5.5 Butir uji pengujian tahap 2 memasukkan kata kunci .....	V-11
5.6 Butir uji pengujian tahap 3 mengambil pesan teks dalam citra digital .....	V-12
5.7 Hasil pengujian penyembunyian data. ....	V-14
5.8 Hasil pengujian ekstraksi data pesan. ....	V-15
5.9 Perbandingan ukuran berkas asli dengan berkas hasil steganografi. ....	V-15
5.10 Pengujian pemotongan ( <i>Cropping</i> ) .....	V-16
5.11 Pengujian pemutaran ( <i>Rotate</i> ) .....	V-17
5.12 Pengujian perubahan ukuran ( <i>Resize</i> ) .....	V-19

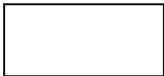
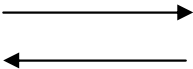

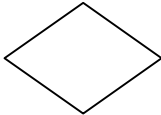



## DAFTAR ISTILAH

<b><i>Binary image</i></b>	= Citra digital yang setiap <i>pixel</i> -nya hanya memiliki 2 kemungkinan nilai, yaitu 0 dan 1
<b><i>Bit</i></b>	= Satuan terkecil dalam hitungan biner
<b><i>Bitmap</i></b>	= Gambar grafis komputer yang terdiri atas titik-titik yang membentuk baris dan kolom.
<b><i>Byte</i></b>	= Satuan dari penyimpanan data dalam komputer yang terdiri dari delapan <i>bit</i> .
<b><i>Cover object</i></b>	= Media penampung pesan
<b><i>De-spreading</i></b>	= Penyusutan data atau informasi
<b><i>Encoding</i></b>	= Penyandian
<b><i>Exclusive OR (XOR)</i></b>	= Salah satu Gerbang Logika yang outputnya akan bernilai <i>TRUE</i> jika salah satu dari dua inputnya bernilai <i>TRUE</i> .
<b><i>Fidelity</i></b>	= Mutu media penampung tidak berubah banyak akibat penyisipan
<b><i>Flowchart</i></b>	= Aliran Proses atau data
<b><i>Graptos</i></b>	= Catatan atau Tulisan
<b><i>Grayscale</i></b>	= Citra keabuan
<b><i>Grid</i></b>	= Garis bantu.
<b><i>Hardware</i></b>	= Perangkat keras
<b><i>Imperceptibility</i></b>	= Keberadaan pesan tidak dapat dipersepsi oleh indrawi
<b><i>Input</i></b>	= Data yang dimasukkan
<b><i>Least Significant Bit</i></b>	= Angka yang memiliki bobot paling kecil dalam susunan bilangan biner.
<b><i>Lossy compression</i></b>	= Tidak tahan terhadap proses kompresi

<b><i>Monochrome</i></b>	= Citra digital yang setiap <i>pixel</i> -nya hanya memiliki 2 kemungkinan nilai, yaitu 0 dan 1
<b><i>Most Significant Bit</i></b>	= Angka yang paling berarti atau paling besar nilainya
<b><i>Pixel</i></b>	= <i>Picture element</i> , Elemen terkecil citra digital yang bisa dilihat mata.
<b><i>Pseudo-noise signal</i></b>	= Bilangan semu acak yang dapat diungkapkan kembali
<b><i>Recovery</i></b>	= Pengungkapan kembali
<b><i>Software</i></b>	= Perangkat lunak
<b><i>Spreading</i></b>	= Penyebaran data atau informasi
<b><i>Steganos</i></b>	= Tersembunyi atau Disembunyikan
<b><i>Stego Image</i></b>	= Berkas Citra digital yang telah disisipi pesan
<b><i>Stego key</i></b>	= Kata kunci yang digunakan dalam proses steganografi
<b><i>True color</i></b>	= Citra warna
<b><i>User</i></b>	= Pengguna
<b><i>User Interface</i></b>	= Tampilan antar muka pemakai
<b><i>Watermark</i></b>	= Cara penyembunyian atau penanaman data atau informasi tertentu.

## DAFTAR SIMBOL

Simbol	Keterangan Simbol
	Proses pada bagan alir sistem pada <i>flowchart</i>
	Aliran proses pada bagan alir sistem
	Terminator untuk memulai atau mengakhiri suatu proses pada Bagan Alir Sistem
	Keputusan pada Flowchart
	Simbol yang menyatakan masukan atau keluaran pada <i>flowchart</i>

# BAB I

## PENDAHULUAN

### 1.1 Latar belakang

Perkembangan Teknologi informasi saat ini telah memberikan kemudahan dalam melakukan aktivitas manusia. Pengiriman data dan informasi menjadi lebih mudah dan cepat. Seiring dengan perkembangan teknologi informasi tersebut, semakin berkembang pula teknik kejahatan yang berupa perusakan maupun pencurian data oleh pihak yang tidak memiliki wewenang atas data tersebut. Dengan berbagai teknik pengambilan informasi secara ilegal yang berkembang, banyak yang mencoba untuk mengakses informasi yang bukan haknya. Oleh karena itu, pada saat ini telah dilakukan berbagai upaya untuk menjaga keamanan data dan informasi tersebut.

Berbagai macam teknik digunakan dalam upaya mengamankan suatu data penting. Sebelumnya telah ada cara untuk menjaga keamanan data yang dikenal dengan nama kriptografi. Dengan kriptografi data rahasia terjaga keamanannya, namun bentuk *chipertext* yang diacak akan mudah terdeteksi dan menyadarkan pihak ketiga akan kerahasiaan file tersebut. Untuk itu diterapkan steganografi (*covered writing*) dalam usaha menjaga kerahasiaan data.

Pada Tugas Akhir ini akan dibahas steganografi menggunakan wadah penampung berupa citra digital. Penggunaan wadah penampung berupa citra digital karena adanya batasan kepekaan manusia dalam hal visualisasi. Hasil keluaran citra digital dari steganografi ini memiliki bentuk persepsi yang sama dengan aslinya, tentunya persepsi disini sebatas kemampuan indera manusia, tetapi tidak oleh komputer atau pengolah digital lainnya.

Metode yang digunakan dalam steganografi ini adalah metode *Spread spectrum* dalam pengacakan pesan dan menggunakan metode Modifikasi LSB (*Least Significant Bit*) dalam menyisipkan pesan rahasia ke media citra digital.

Modifikasi LSB dilakukan dengan mengganti bit-bit data yang kurang berarti di dalam segmen citra dengan bit-bit pesan rahasia.

Steganografi pada citra digital dapat dijadikan alternatif untuk menyimpan data rahasia ke dalam wadah citra digital. Steganografi dapat juga digunakan untuk menyampaikan pesan rahasia, karena sifat dari steganografi yang sulit dideteksi keberadaannya. Dalam bidang keamanan komputer, steganografi digunakan untuk menyembunyikan data rahasia pada saat proses enkripsi tidak dapat dilakukan atau bersamaan dengan proses enkripsi.

Berdasarkan permasalahan diatas maka akan dibuat aplikasi steganografi pada citra digital dengan metode *spread spectrum* dalam pengacakan pesannya dan metode modifikasi LSB dalam menyisipkan pesan yang sudah diacak.

## **1.2 Rumusan masalah**

Rumusan masalah dari tugas akhir ini adalah: Bagaimana menerapkan metode *Spread Spectrum* dan Metode *Least Significant Bit (LSB) Modification* dalam steganografi pada citra digital

## **1.3 Batasan masalah**

Batasan masalah dalam Tugas Akhir ini adalah:

1. Berkas citra digital yang digunakan untuk menyembunyikan data pesan adalah berkas citra warna (RGB) berformat *Bitmap* (\*.bmp)
2. Data Pesan yang disisipkan adalah data pesan teks dan berkas dokumen.
3. Dalam penyisipan data pesan, Bit yang digunakan pada wadah citra digital hanya bit yang paling akhir (paling kanan) dalam setiap *byte*.

## **1.4 Tujuan**

Tujuan yang ingin dicapai dalam penyusunan tugas akhir ini adalah membuat suatu aplikasi Steganografi menggunakan metode *spread spectrum* dan metode *Least Significant Bit (LSB) Modification* ke dalam file citra digital.

## **1.5 Sistematika Penulisan**

Sistematika penulisan laporan tugas akhir terbagi dalam 6 (enam) bab. Berikut penjelasan dari masing-masing bab.

### **BAB I : PENDAHULUAN**

Menjelaskan dasar-dasar dari penulisan laporan tugas akhir ini, yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan serta sistematika penulisan laporan tugas akhir.

### **BAB II : LANDASAN TEORI**

Menjelaskan teori-teori tentang Steganografi, *Spread spectrum*, Citra Digital dan teori pendukung yang berkaitan dengan tugas akhir yang akan dibuat.

### **BAB III : METODOLOGI PENELITIAN**

Metodologi penelitian merupakan langkah sistematis dan logis yang disusun secara tahap demi tahap pengerjaan selama pembuatan sistem. Seperti penelitian pendahuluan, identifikasi masalah, penetapan tujuan, pengumpulan data, analisa sistem, perancangan sistem, implementasi dan pengujian, serta kesimpulan dan saran.

### **BAB IV : ANALISA DAN PERANCANGAN**

Bab ini membahas hasil analisa dan perancangan yang meliputi pembahasan mengenai deskripsi metode, analisa perangkat lunak dan perancangan perangkat lunak.

## BAB V : IMPLEMENTASI DAN PENGUJIAN

Bab ini membahas implementasi, pengujian, deskripsi pengujian, pengujian berdasarkan kriteria steganografi dan kesimpulan pengujian.

## BAB VI : KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran sebagai hasil akhir dari penelitian tugas akhir yang telah dilakukan.

## **BAB II**

### **LANDASAN TEORI**

Landasan teori disusun berdasarkan teori-teori mengenai metode yang digunakan dalam steganografi dan penjelasan tentang media penyimpanan pesan yang akan disembunyikan, yang diperoleh dari beberapa referensi buku dan internet.

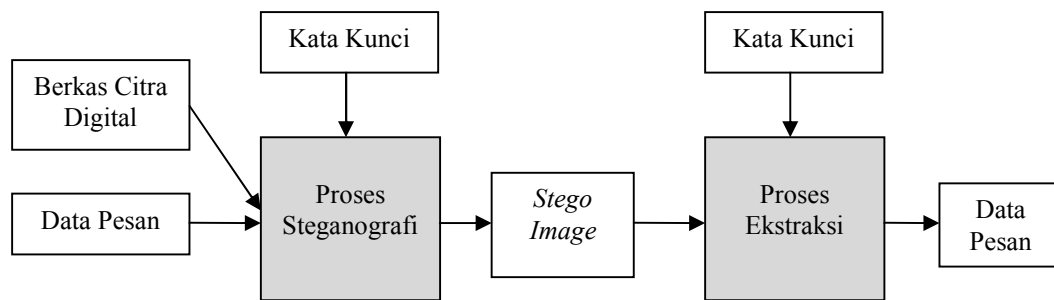
#### **2.1 Steganografi**

Steganografi berasal dari bahasa Yunani yaitu *Steganós* yang berarti menyembunyikan dan *Graptos* yang artinya tulisan, sehingga secara keseluruhan artinya adalah tulisan yang disembunyikan. Secara umum steganografi adalah ilmu dan seni menyembunyikan pesan rahasia sedemikian sehingga keberadaan pesan tidak terdeteksi oleh indera manusia.

Steganografi sangat kontras dengan kriptografi. Kriptografi merahasiakan makna pesan sementara eksistensi pesan tetap ada, sedangkan steganografi menutupi keberadaan pesan. Steganografi dapat dipandang sebagai kelanjutan dari kriptografi.

Dalam prakteknya, pesan diacak terlebih dahulu, kemudian disembunyikan di dalam media lain sehingga pihak ketiga tidak menyadari keberadaan pesan. Steganografi membutuhkan dua properti, yaitu pesan dan media penampung. Media penampung yang umumnya digunakan sekarang dapat berupa teks, suara, gambar, atau video. Sedangkan pesan yang disembunyikan dapat berupa teks, gambar, atau pesan lainnya. (Novrina, 2008)





Gambar 2.1. Model sistem Steganografi

Keuntungan penggunaan steganografi adalah memungkinkan pengiriman pesan secara rahasia tanpa diketahui bahwa pesan sedang dikirim. Ini membuat pihak ketiga tidak menyadari keberadaan pesan. Sebaliknya, penggunaan kriptografi akan menarik kecurigaan pihak ketiga bahwa ada sesuatu yang disembunyikan dalam pesan yang sedang dikirim.

Steganografi juga memiliki kelemahan. Tidak seperti kriptografi, steganografi memerlukan banyak ruang untuk dapat menyembunyikan beberapa bit pesan. Akan tetapi, kelemahan ini sedikit demi sedikit dapat diatasi seiring dengan perkembangan teknik-teknik dalam melakukan steganografi.

Dalam menyembunyikan pesan, ada beberapa kriteria yang harus dipenuhi, diantaranya adalah:

1. **Imperceptibility**. Keberadaan pesan tidak dapat dipersepsi oleh indrawi. Jika pesan disisipkan ke dalam sebuah citra, citra yang telah disisipi pesan harus tidak dapat dibedakan dengan citra asli oleh mata. Begitu pula dengan suara, telinga haruslah mendapati perbedaan antara suara asli dan suara yang telah disisipi pesan.
2. **Fidelity**. Mutu media penampung tidak berubah banyak akibat penyisipan. Perubahan yang terjadi harus tidak dapat dipersepsi oleh indra manusia.
3. **Recovery**. Pesan yang disembunyikan harus dapat diungkap kembali. Tujuan steganografi adalah menyembunyikan informasi, maka sewaktu-waktu informasi yang disembunyikan ini harus dapat diambil kembali untuk dapat digunakan lebih lanjut sesuai keperluan.

### 2.1.1 Sejarah Steganografi

Catatan tertua mengenai penggunaan steganografi tercatat pada masa Yunani kuno. Pada saat itu, penguasa Yunani, Histiaues, sedang ditawan oleh Raja Darius di Susa. Histiaeus ingin mengirim pesan rahasia kepada menantunya, Aristagoras, di Miletus. Untuk itu, Histiaeus mencukur habis rambut budaknya dan menatoken pesan rahasia yang ingin dikirim di kepala budak tersebut. Setelah rambut budak tadi tumbuh cukup lebat, barulah ia dikirim ke Miletus.

Cerita lain masih juga berasal dari zaman Yunani kuno. Medium tulisan pada saat itu adalah papan yang dilapisi lilin dan tulisan ditulis di papan tersebut. Demeratus, perlu memberitahu Sparta bahwa Xerxes bermaksud untuk menginvasi Yunani. Agar pesan yang dikirimnya tidak diketahui keberadaannya, Demeratus melapisi lagi papan tulisannya dengan lilin. Papan tulisan yang terlihat masih kosong inilah yang dikirim ke Sparta. Tinta yang tidak nampak merupakan salah satu metode yang populer dalam bidang steganografi.

Bangsa Romawi telah menggunakan tinta yang tidak nampak ini untuk menulis pesan di antara baris-baris pesan yang ditulis dengan tinta biasa. Tinta yang tidak nampak ini dapat terbuat dari sari jeruk atau susu. Ketika dipanaskan, warna tinta yang tidak tampak akan menjadi gelap dan tulisannya akan menjadi dapat terbaca. Tinta yang tidak tampak ini juga digunakan dalam Perang Dunia II.

Steganografi terus berkembang selama abad kelima belas dan keenam belas. Pada masa itu, banyak penulis buku yang enggan mencantumkan namanya karena takut akan kekuatan penguasa pada saat itu. Pengembangan lebih jauh lagi mengenai steganografi terjadi pada tahun 1883 dengan dipublikasikannya kriptografi militer oleh Auguste Kerckhoffs.

Meskipun sebagian besar berbicara mengenai kriptografi, Kerckhoffs menjabarkan beberapa deskripsi yang patut dicatat ketika merancang sebuah sistem steganografi. Lebih jauh lagi, *Les Filigranes*, yang ditulis oleh Charle Briquet di tahun 1907, merupakan sebuah kamus sejarah dari *watermark*, salah

satu wujud pengaplikasian steganografi. Dengan adanya komputer, steganografi memperoleh kemajuan yang sangat pesat. Penyembunyian pesan memasuki era baru berkat adanya komputer. (Masaleno, 2006)

### **2.1.2 Manfaat Steganografi**

Steganografi dapat digunakan untuk menyembunyikan informasi rahasia ke dalam media lain, untuk melindunginya dari pencurian dan dari orang-orang yang tidak berhak untuk mengetahuinya. Steganografi juga dapat digunakan untuk pengiriman pesan secara rahasia tanpa diketahui bahwa pesan sedang dikirim. Ini membuat pihak ketiga tidak menyadari keberadaan pesan.

Di sisi lain steganografi juga bisa digunakan sebagai sarana kejahatan. Steganografi dapat digunakan untuk mencuri data yang disembunyikan pada data lain sehingga dapat dikirim ke pihak lain tanpa ada yang curiga. Steganografi juga dapat digunakan oleh para teroris untuk saling berkomunikasi dengan yang lain.

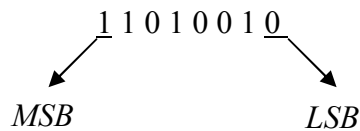
### **2.1.3 Metode Steganografi**

Steganografi dapat diterapkan pada data digital, yaitu teks, citra, suara dan video. Terdapat banyak metode steganografi untuk citra digital yang sudah ada. Ada yang bekerja pada *domain spasial* atau waktu seperti metode Modifikasi LSB (*Least Significant Bit*) dan ada yang mengalami transformasi terlebih dahulu, misalnya ke domain frekuensi seperti DCT (*Domain Cosine Transform*), *Wavelet Transform*, *Spread Spectrum*, dan sebagainya.

#### **2.1.3.1. Modifikasi LSB (*Least Significant Bit Modification*)**

Cara paling umum untuk menyembunyikan pesan adalah dengan memanfaatkan *Least-Significant Bit* (LSB). Kemudahan implementasinya membuat metode ini tetap digunakan sampai sekarang. Metode ini membutuhkan syarat, yaitu jika dilakukan kompresi pada *stego*, harus digunakan *format lossless compression*, karena metode ini menggunakan *bit-bit* setiap *piksel* pada *image*.

Penyembunyian data dilakukan dengan mengganti beberapa *bit data* di dalam *biner data* dengan *bit-bit data* rahasia. Pada susunan *bit* di dalam sebuah *byte* (1 *byte* = 8 *bit*), ada *bit* yang paling berarti (*Most Significant Bit*) dan *bit* yang paling kurang berarti (*Least Significant Bit*).



*Bit* yang cocok untuk diganti adalah *bit LSB*, karena perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan *byte* tersebut menyatakan warna merah, maka perubahan satu *bit LSB* tidak mengubah warna merah tersebut secara berarti. Lagi pula, indra penglihatan manusia tidak dapat membedakan perubahan yang kecil.

Jika digunakan format *lossy compression*, pesan rahasia yang disembunyikan dapat hilang. Jika digunakan *image 24 bit color* sebagai *cover*, sebuah *bit* dari masing-masing komponen *Red*, *Green*, dan *Blue*, dapat digunakan sehingga 3 *bit* dapat disimpan pada setiap *piksel*. Sebuah *image* 800 x 600 *piksel* dapat digunakan untuk menyembunyikan 1.440.000 *bit* (180.000 bytes) data rahasia.

Adapun keuntungan dari pemanfaatan metode *LSB* adalah sebagai berikut:

1. Keuntungan yang paling besar dari algoritma *LSB* ini adalah mudah diimplementasikan dan proses *encoding* cepat.
2. Dan juga algoritma tersebut memiliki software steganography yang mendukung dengan bekerja diantara unsur pokok warna *LSB* melalui manipulasi palette (lukisan).
3. Mengubah *bit LSB* hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya, sehingga tidak berpengaruh terhadap persepsi visual/auditori.

Selain dari beberapa kelebihan diatas, metode *LSB* juga memiliki kekurangan sebagai berikut:

1. Tidak tahan terhadap perubahan (modifikasi) terhadap *cover object*. Menggunakan *LSB Insertion* dapat secara drastis merubah unsur pokok warna dari pixel. sehingga tanda tersebut menunjukkan keberadaan dari steganografi.
2. Mudah dihapus karena lokasi penyisipan diketahui (bit *LSB*)

#### **2.1.3.2 Spread Spectrum**

Metode *spread spectrum* dalam steganografi diilhami dari skema komunikasi *spread spectrum*, yang mentransmisikan sebuah sinyal pita sempit ke dalam sebuah kanal pita lebar dengan penyebaran frekuensi. *Spread Spectrum* steganography terpecah-pecah sebagai pesan yang diacak (*encrypt*) melalui gambar. Untuk membaca suatu pesan, penerima memerlukan algoritma yaitu *crypto-key* dan *stego-key*. Metode ini juga masih mudah diserang yaitu penghancuran atau pengrusakan dari kompresi dan proses *image* (gambar)

Pada proses penyembunyian data, bit-bit informasi yang telah mengalami proses *spreading* ini kemudian akan dimodulasi dengan *pseudo-noise signal* yang dibangkitkan secara acak berdasarkan kunci penyembunyian. Hasil dari proses modulasi ini kemudian digabungkan sebagai *noise* ke dalam sebuah berkas media pada bit-bit terakhir dari berkas media. .

Oleh penerima, sinyal dikumpulkan kembali menggunakan replika *pseudo-noise signal* tersinkronisasi. Media yang telah berisi informasi rahasia tersebut disaring terlebih dahulu dengan proses *pre-filtering* untuk mendapatkan *noise*. *Noise* yang dihasilkan selanjutnya dimodulasi dengan menggunakan *pseudo-noise signal* untuk mendapatkan bit-bit yang berkorelasi. Bit-bit yang berkorelasi tersebut dianalisa dengan perhitungan tertentu untuk menghasilkan bit-bit informasi yang sesungguhnya.

Berdasarkan definisi, dapat dikatakan bahwa steganografi menggunakan metode *spread spectrum* memperlakukan *cover-object* baik sebagai derau (*noise*) ataupun sebagai usaha untuk menambahkan derau semu (*pseudo-noise*) ke dalam *cover-object*. *Cover-object* sebagai derau Sistem yang memperlakukan *cover-object* sebagai derau dapat menambahkan sebuah nilai ke dalam *cover-object*. Nilai ini harus ditransmisikan di bawah tingkat derau yang ditambahkan nilai ke dalamnya. Hal ini berarti kapasitas sangat ditentukan oleh *cover-object*. (

## **2.2 Citra Digital**

Citra digital dapat dibedakan menjadi dua, yaitu *raster* dan *vektor*. Pada umumnya, yang disebut dengan citra digital adalah citra digital dalam bentuk *raster* atau yang biasa disebut dengan citra bitmap.

### **2.2.1 Konsep dasar citra digital**

Citra digital tersusun dalam bentuk *raster* (*grid* atau kisi). Setiap kotak yang terbentuk disebut *pixel* (*picture element*) dan memiliki koordinat (x,y). Koordinat ini biasanya dinyatakan dalam bilangan bulat positif. Dan setiap *pixel* memiliki nilai berupa angka digital yang merepresentasikan informasi yang diwakili oleh *pixel* tersebut.

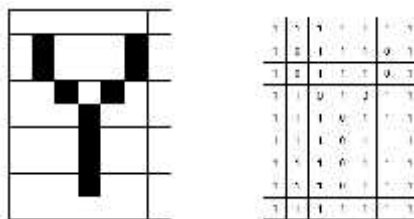
Representasi citra digital dalam sebuah file dapat dianalogikan seperti halnya ketika kita ingin melukis, maka kita harus mempunyai palet dan kanvas. Di mana palet adalah kumpulan warna yang dapat membentuk citra, seperti palet warna yang berisi berbagai warna cat. Lalu setiap warna yang berbeda di dalam palet tersebut diberi nomor. Kemudian kita dapat melukiskan warna-warna tersebut di atas sebuah kanvas. Kanvas tersebut berupa matriks yang setiap elemen matriksnya dapat diisi dengan sebuah warna yang berasal dari palet warna. Kumpulan angka (mewakili warna) dalam bentuk matriks inilah yang disebut dengan citra.

### 2.2.2 Jenis citra digital

Jenis citra digital berhubungan erat dengan warna. Nilai data digital merepresentasikan warna dari citra. Format citra digital yang banyak digunakan adalah citra biner (*monochrome*), citra skala keabuan (*gray scale*), citra warna (*true color*), dan citra warna berindeks.

#### 2.2.2.1. Citra biner (*Monochrome*)

Citra biner (*monochrome*) atau disebut juga *binary image*, merupakan citra digital yang setiap *pixel*-nya hanya memiliki 2 kemungkinan derajat keabuan, yaitu 0 dan 1. Nilai 0 mewakili warna hitam, dan nilai 1 mewakili warna putih, di mana setiap *pixel*-nya membutuhkan media penyimpanan sebesar 1 bit.



1	0	1	0	0	0	1
1	0	1	1	0	0	1
1	0	1	1	1	0	1
1	0	0	1	0	1	1
1	0	1	0	0	0	1
1	0	1	0	0	0	1
1	0	1	0	0	0	1
1	0	1	0	0	0	1
1	0	1	0	0	0	1

Gambar 2.2 Contoh Citra Biner Berukuran 9x7 Pixel dan Representasinya dalam Data Digital



Gambar 2.3 Contoh Citra Biner

#### 2.2.2.2. Citra skala keabuan (*grayscale*)

Citra skala keabuan atau disebut juga dengan citra aras keabuan memberikan kemungkinan warna yang lebih banyak. Format citra ini disebut

dengan aras keabuan karena ada warna abu-abu diantara warna minimum (hitam) dan warna maksimum (putih). Jumlah maksimum warna sesuai dengan bit penyimpanan yang digunakan, apakah 4 bit atau 8 bit. Citra dengan skala keabuan 4-bit memiliki  $2^4 = 16$  kemungkinan warna, yaitu 0 (minimal) hingga 15 (maksimal). Sementara citra digital dengan skala keabuan 8-bit memiliki  $2^8 = 256$  kemungkinan warna, yaitu 0 (minimal) hingga 255 (maksimal).



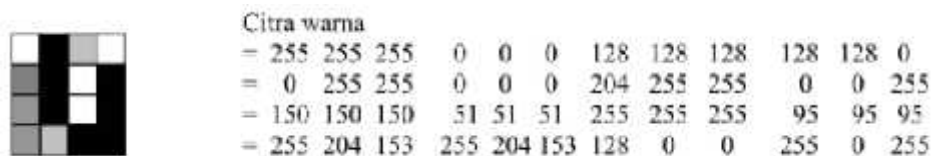
Gambar 2.4 Citra Skala Keabuan 4-Bit dan Representasinya dalam Data Digital



Gambar 2.5 Contoh Citra Skala Keabuan 8-Bit

### 2.2.2.3. Citra warna (*true color*)

Pada citra warna (*true color*) setiap *pixel*-nya merupakan kombinasi dari tiga warna dasar merah, hijau, dan biru, sehingga citra warna ini disebut juga citra RGB (*Red Green Blue*). Setiap komponen warna memiliki intensitas sendiri dengan nilai minimum 0 dan nilai maksimum 255 (8-bit). Hal ini menyebabkan setiap pixel pada citra RGB membutuhkan media penyimpanan 3 byte. Jumlah kemungkinan kombinasi warna citra RGB adalah  $2^{24}$  = lebih dari 16 juta warna.







*Gambar 2.6 Contoh Citra Warna dan Representasinya dalam Data Digital*

### **2.2.3 Citra *Bitmap***

*Bitmap* adalah representasi dari citra grafis yang terdiri dari susunan titik yang tersimpan di memori komputer. Dikembangkan oleh *Microsoft* dan nilai setiap titik diawali oleh satu bit data untuk gambar hitam putih, atau lebih bagi gambar berwarna. Kerapatan titik-titik tersebut dinamakan resolusi, yang menunjukkan seberapa tajam gambar ini ditampilkan, ditunjukkan dengan jumlah baris dan kolom.

Tipe file ini biasanya digunakan pada sistem operasi *Windows* dan *OS/2*. Kelebihan tipe file *BMP* adalah dapat dibuka oleh hampir semua program pengolah gambar. Baik file *BMP* yang terkompresi maupun tidak terkompresi, *file BMP* memiliki ukuran yang jauh lebih besar daripada tipe-tipe yang lain. Kelebihan citra *Bitmap* ialah mendukung penggunaan warna 1bit hingga 32 bit. *Bitmap* cocok untuk gambar-gambar seperti desain logo, *banner* dan sebagainya. Sedangkan kekurangan citra *bitmap* ialah ukuran yang lebih besar daripada citra format lain.

Pada representasi *bitmap*, sebuah citra dibagi menjadi kotak-kotak berukuran kecil dimana setiap kotak menyimpan nilai intensitas warna yang disebut *pixel*.

Adapun format detail dari citra *bitmap* adalah terdiri dari:

1. Header Informasi *Bitmap*.
2. Tabel Warna.
3. Data *Bitmap*.

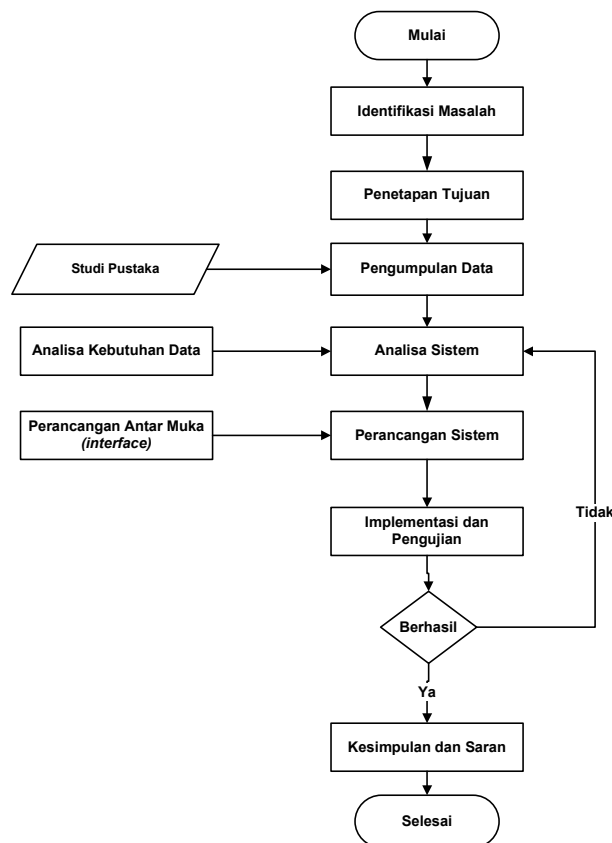
Pada umumnya, file citra *bitmap* memiliki *resolusi* yaitu 1, 4, 8 dan 24 bits per *pixel*, tapi dalam tugas akhir ini hanya menggunakan 24 *bits* sebagai bentuk citra yang umum, dan citra 24 *bits* penanganannya sama dengan dengan citra 8 *bits*, dalam artian nilai intensitas warnanya akan diterjemahkan ke dalam representasi yang sama dengan 8 *bits*. Untuk citra 24 *bits* tidak menggunakan tabel warna sedangkan untuk citra 1, 4, 8 bit harus memiliki tabel warna *palette* yang ukuran maksimumnya masing-masing adalah 2, 16 dan 256 *entry*, dimana masing-masing *entry* merupakan warna *RGB*.

Tipe data yang paling berperan dalam system ini adalah *RGB*. Tipe ini digunakan untuk melakukan manipulasi sebuah *pixel* pada citra. *RGB* merupakan *record* yang mempunyai tiga anggota yaitu *rgbred*, *rgbgreen*, *rgbblue* yang secara berurutan merepresentasikan nilai *RGB* suatu *pixel*. (Putra, 2010)

### BAB III

## METODOLOGI PENELITIAN

Metodologi adalah tatacara yang disusun secara pasti, sistematis dan logis sebagai landasan untuk suatu kegiatan tertentu. Metodologi yang diperlukan untuk tugas akhir ini terdiri dari beberapa tahap seperti: Tahap pengumpulan data, tahap analisa dan perancangan, tahap implementasi dan tahap pengujian. Gambar 3.1 menunjukkan langkah-langkah metodologi pengembangan perangkat lunak Steganografi pada citra digital menggunakan metode *spread spectrum* dalam pengacakan pesan dan modifikasi LSB (*Least Significant Bit Modification*) dalam menyisipkan pesan yang sudah diacak ke dalam file citra digital.



Gambar 3.1 Langkah-langkah metodologi penelitian

### **3.1 Identifikasi Masalah**

Pada tugas akhir ini, masalah penelitian secara umum bisa kita temukan lewat studi literatur atau lewat pengamatan lapangan, selanjutnya barulah dilakukan pengidentifikasian masalah. Adapun masalah yang akan diidentifikasi adalah yaitu bagaimana menerapkan metode *Spread Spectrum* dan Metode *Least Significant Bit (LSB) Modification* dalam steganografi pada citra digital.

### **3.2 Penetapan Tujuan**

Penetapan tujuan sangat diperlukan untuk menjawab permasalahan yang ada. Penetapan tujuan dilakukan setelah mengidentifikasi masalah. Tujuan akan ditetapkan dengan cara mengetahui dan menentukan apa saja yang perlu dipertahankan, ditingkatkan, dihilangkan, dievaluasi dan diperbarui dari suatu masalah yang ada dapat teratasi.

### **3.3 Pengumpulan Data**

Tahapan ini merupakan langkah-langkah yang dilakukan untuk mendapatkan data yang dibutuhkan, yaitu dengan membaca buku-buku yang berhubungan dengan steganografi, metode *spread spectrum*, *least significant bit (LSB) Modification*, teori citra digital, serta mencari informasi dan literatur dari internet.

### **3.4 Analisa Sistem**

Pada tahap ini dilakukan analisa data dan permasalahan yang telah dirumuskan, kemudian merancang sebuah sistem yang dapat menjawab permasalahan dan kendala yang ada. Adapun analisa yang dilakukan adalah:

Analisa setelah data yang dikumpulkan telah lengkap agar selanjutnya mulai merancang sebuah sistem yang dapat menjawab permasalahan dan kendala yang ada. Pada saat menganalisa data, ada beberapa tahap yang harus dilakukan, yaitu mengidentifikasi kebutuhan sistem, fungsi sistem, memodelkan sistem yang akan dibangun, karakteristik pengguna, merancang lingkungan implementasi, serta merancang antar muka pengguna sistem yang akan dibangun. Perancangan

antar muka pengguna sistem digunakan untuk memudahkan tahap implementasi pada saat membangun antar muka pengguna.

Tahapan analisa menentukan bagaimana implementasi harus dikerjakan, dan pada tahapan perancangan menentukan bagaimana pemecahan masalah akan dikerjakan atau bagaimana melakukannya

### **3.5 Perancangan Sistem**

Tujuan dari perancangan sistem ini adalah bagaimana mengimplementasikan permasalahan yang ada kedalam sebuah program dan memberikan gambaran komponen-komponen sistem secara umum kepada pengguna sistem tentang sistem yang akan dibuat.

Tahap-tahap yang dilakukan dalam perancangan ini adalah sebagai berikut:

1. Perancangan antarmuka
2. Perancangan menu

### **3.6 Implementasi dan Pengujian**

Tahapan implementasi merupakan tahap dimana sistem siap dioperasikan pada keadaan yang sebenarnya, sehingga akan diketahui apakah sistem yang dibuat benar-benar dapat menghasilkan tujuan yang ingin dicapai.

Dalam implementasi dan pengujian ini akan digunakan:

1. Perangkat lunak dan perangkat keras.

Lingkungan implementasi sistem ada dua, yaitu lingkungan perangkat keras (*Hardware*) dan perangkat lunak (*Software*).

2. *Coding*

Pembuatan coding program dilakukan menggunakan program *Visual Basic*.

Kumpulan dari semua program yang telah diintegrasikan perlu dites kembali untuk melihat apakah suatu program dapat menerima masukan data dengan baik, dapat memprosesnya dengan baik dan dapat memberikan *output* kepada program lainnya.

### **3.7 Kesimpulan dan Saran**

Kesimpulan merupakan hasil akhir yang didapat dari pembahasan sesuai dengan proses yang telah dilakukan sebelumnya. Kesimpulan yang diambil dapat bersifat positif maupun negatif yang ditinjau dari berbagai aspek. Saran merupakan sesuatu yang diharapkan di masa mendatang bagi perkembangan sistem selanjutnya.

## BAB IV

### ANALISA DAN PERANCANGAN

Teknik yang akan digunakan untuk implementasi steganografi pada citra digital ini adalah teknik *spread spectrum* terhadap pesan yang akan disembunyikan. Metode ini menyebarkan sinyal dengan melipatgandakannya, untuk selanjutnya dimodulasi dengan chip dari kunci. Besaran skalar faktor pengali pelipatgandaan ini ditentukan secara tetap oleh sebuah konstanta. *Pseudo-noise signal* digunakan untuk mengacak pesan. Metode penyisipan data pesan ke dalam citra digital menggunakan metode modifikasi LSB terhadap data gambar.

#### 4.1. Deskripsi Metode

Metode steganografi ini membutuhkan 3 data masukan untuk memulai proses, yaitu berkas citra digital, data pesan rahasia, dan kunci. Ketiga data masukan itu dibutuhkan pada metode pembangkitan *pseudo-noise*, metode *spread spectrum*, metode penyisipan serta metode ekstraksi.

##### 4.1.1 Deskripsi Metode Penyisipan

Proses pertama terhadap pesan rahasia dalam metode *spread spectrum* adalah dengan melakukan proses *spreading*. Misalkan suatu segmen pesan rahasia adalah '1 0 1 0', maka setelah proses *spreading* dengan besaran skalar pengalinya 4, akan menghasilkan segmen baru yaitu:

' 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 '

Terlihat bahwa setiap bit dalam segmen pesan akan mengalami penggandaan bit sebanyak 4 kali dan ukuran segmen pesan menjadi lebih panjang 4 kali ukuran semula.

Proses selanjutnya terhadap pesan ini adalah dengan proses modulasi, yaitu mengacaknya dengan suatu *pseudo-noise signal* yang dibangkitkan. pembangkitan *pseudonoise signal* ini menggunakan bilangan *pseudonumber* yang diambil dari variabel kunci.

Misalkan dari hasil pembangkitan, diperoleh *pseudo-noise signal* sebagai berikut:

'01110100000010010000110111110000'

Selanjutnya segmen pesan akan dimodulasi dengan *pseudo-noise signal* menggunakan fungsi *XOR (Exclusive OR)*.

Segmen pesan:

'11110000111111110000000011110000'

*Pseudo-noise:*

'01110100000010010000110111110000'

Hasil:

'10000100111101100000110100000000'

Hasil dari proses modulasi inilah yang kemudian akan disisipkan ke dalam *bit-bit LSB* pada berkas citra digital. Metode penyisipan yang dipilih adalah modifikasi *LSB* terhadap media citra digital.

Dalam menyisipkan data pesan ke dalam berkas citra digital menggunakan metode *Least Significant Bit (LSB) Modification*. Misalkan untuk menyisipkan suatu segmen pesan hasil dan modulasi sebesar 4 *byte* dengan modifikasi 1 bit *LSB*, maka dibutuhkan 32 data citra digital untuk menampungnya. dari segmen pesan '1010' dengan 4 *byte* data citra digital sebagai berikut:

'01101110 00100011 01000010 01101101'

Maka dengan operasi penggantian bit terakhir dengan 4 bit segmen pesan secara berurutan menjadi sebagai berikut:

Data citra digital:

'01101110 00100011 01000010 01101101'

Pesan:

1 0 1 0

Hasil:

'01101111001000100100001101101100'



Dengan sedikit modifikasi ini, maka efek dari perubahan nilai warna yang terjadi akibat perubahan *bit* tersebut tidak terlalu berpengaruh terhadap kualitas gambar.

#### 4.1.2 Deskripsi Metode Ekstraksi

Proses dalam metode ekstraksi adalah kebalikan dari proses dalam metode penyisipan. Pertama-tama berkas citra digital yang berisi pesan, akan di-*parsing* dengan berurutan sebagai berikut :

0 1 1 0 1 1 1 1    0 0 1 0 0 0 1 0    0 1 0 0 0 0 1 0    0 1 1 0 1 1 0 0

maka hasil penyaringan *bit-bit* terakhirnya adalah ' 1 0 0 0 '. Setiap bit terakhir atribut *velocity* ini akan di-demodulasi dengan *pseudo-noise signal* yang dihasilkan yang sama dengan metode penyembunyian.

Proses demodulasi terhadap *bit-bit LSB* atribut berkas citra digital dengan *pseudo-noise* ini menggunakan fungsi *XOR*. Hasilnya adalah pesan dalam bentuk yang tersebar dengan faktor pengali tertentu. Contoh bila hasil penyaringan *bit-bit* terakhir adalah

' 1 0 0 0 0 1 0 0 1 1 1 1 0 1 1 0 0 0 0 0 1 1 0 1 0 0 0 0 0 0 0 0 '

Maka proses *demodulasi* menggunakan *pseudo-noise* yang sama dengan proses penyisipan adalah sebagai berikut:

Hasil penyaringan:

' 1 0 0 0 0 1 0 0 1 1 1 1 0 1 1 0 0 0 0 0 1 1 0 1 0 0 0 0 0 0 0 0 '

*Pseudo-noise:*

' 0 1 1 1 0 1 0 0 0 0 0 0 1 0 0 1 0 0 0 0 1 1 0 1 1 1 1 1 0 0 0 0 '

Hasil demodulasi:

' 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 '

Untuk dapat menghasilkan pesan yang sesungguhnya, maka dibutuhkan proses perhitungan terhadap besaran faktor pengali ini. Faktor pengali yang digunakan sama dengan faktor pengali pada proses *spreading*.

Selanjutnya dilakukan proses *de-spreading* dengan menyusutkan segmen-segmen *bit* yang sama menjadi *bit-bit* yang lebih sederhana. Hasil dari proses *de-spreading* inilah yang dianggap sebagai pesan rahasia sesungguhnya. Contoh bila suatu segmen pesan yang masih tersebar adalah sebagai berikut:

' 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 '

Maka terlihat ada suatu pola pengulangan dari *bit-bit* tersebut, yaitu 4 kali *bit* 1, 4 kali *bit* 0, 8 kali *bit* 1, 8 kali *bit* 0, 4 kali *bit* 1, dan 4 kali *bit* 0. Dengan demikian faktor pengalinya dapat ditentukan besarnya adalah 4 dan proses penyusutan *bit* (*despreading*) segmen tersebut menjadi sebagai berikut:

Sebelum:

' 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 '

Sesudah:

' 1 0 1 1 0 0 1 0 '

Sehingga diperoleh hasil akhir berupa segmen pesan rahasia, yaitu:

' 1 0 1 1 0 0 1 0 '

Hasil ekstraksi ini sama dengan segmen pesan rahasia yang disembunyikan pada metode penyisipan sebelumnya.

## 4.2. Analisa Perangkat Lunak

Dalam Tugas Akhir ini, akan dibangun sebuah perangkat lunak yang mengimplementasikan steganografi pada citra digital. Sebelumnya pernah dilakukan penelitian tentang steganografi pada berkas *Audio WAV* dengan metode *spread spectrum* oleh Dziki Adli (2006). Maka dilakukan pengembangan steganografi pada citra digital dengan metode *Spread Spectrum* dan modifikasi *LSB*. Perangkat lunak ini diberi nama Stegambar (Steganografi pada Gambar).

Untuk selanjutnya perangkat lunak ini disebut demikian dalam pembahasan ini. Analisa perangkat lunak yang akan dibangun meliputi spesifikasi sistem, kebutuhan antarmuka dan kebutuhan fungsional.

#### **4.2.1. Spesifikasi Sistem**

Penjelasan spesifikasi sistem ini mencakup kebutuhan perangkat lunak, tujuan pengembangan perangkat lunak dan arsitektur perangkat lunak.

##### **4.2.1.1 Kebutuhan Perangkat Lunak**

Berdasarkan uraian bab sebelumnya, maka diperlukan suatu perangkat lunak yang dapat memenuhi kebutuhan berikut:

- a. Menerima masukan berkas citra digital asli dan berkas yang telah disisipkan data.
- b. Mampu menyisipkan data ke dalam berkas citra digital.
- c. Menyimpan berkas citra digital yang telah disisipkan data.
- d. Mampu mengekstraksi berkas citra digital yang telah disisipkan data untuk mendapatkan berkas data yang valid.

##### **4.2.1.2 Tujuan Pengembangan Perangkat Lunak**

Pengembangan perangkat lunak Stegambar ditujukan untuk menyisipkan berkas data biner ke dalam berkas gambar atau citra digital dalam format *Bitmap* (*BMP*). Aplikasi Stegambar juga mampu mengekstraksi data yang disisipkan dalam berkas citra digital tersebut.

##### **4.2.1.3. Arsitektur Perangkat Lunak**

Secara garis besar, perangkat lunak Stegambar memiliki dua komponen utama, yaitu komponen penyisipan data ke dalam berkas citra digital dan komponen ekstraksi berkas citra digital yang telah disisipi data. Masukan untuk komponen penyisipan ini adalah sebuah berkas citra digital dengan format *BMP*, data yang akan disisipkan dan sebuah kunci. Keluaran dari komponen ini adalah sebuah berkas citra digital dengan format *BMP* yang telah disisipi data tersebut.

Komponen ekstraksi berkas citra digital melakukan proses ekstraksi kembali berkas citra digital yang telah disisipi data untuk mendapatkan berkas data yang valid. Masukan dari komponen ini adalah sebuah berkas citra digital dengan format *BMP* dan sebuah kunci. Keluaran dari kornponen ini adalah sebuah berkas data yang disisipkan.

#### **4.2.2. Kebutuhan Fungsional**

Model fungsional perangkat lunak memberikan gambaran umum mengenai proses-proses yang terjadi dalam perangkat lunak tanpa memberikan detail mengenai bagaimana proses-proses tersebut diimplementasikan. Model fungsional juga memberikan gambaran tentang aliran data yang terjadi antar proses dan aliran proses dengan entitas luar, misalnya pengguna perangkat lunak.

Aliran data tersebut akan mendefinisikan masukan dan keluaran yang terdapat pada masing-masing proses yang terjadi, sehingga hubungan antar proses terlihat jelas. Aliran informasi, deskripsi proses serta deskripsi data yang termasuk dalam kebutuhan fungsional akan digambarkan dengan alat bantu bagan alur *flowchart*.

Pada diagram ini, proses dilambangkan sebagai lingkaran, sedangkan data masukan dan keluaran tiap proses dilambangkan dengan garis berarah. Arah tersebut menunjukkan arah aliran data antar proses. Entitas luar digambarkan dengan persegi panjang.

### **4.3. Perancangan Perangkat Lunak**

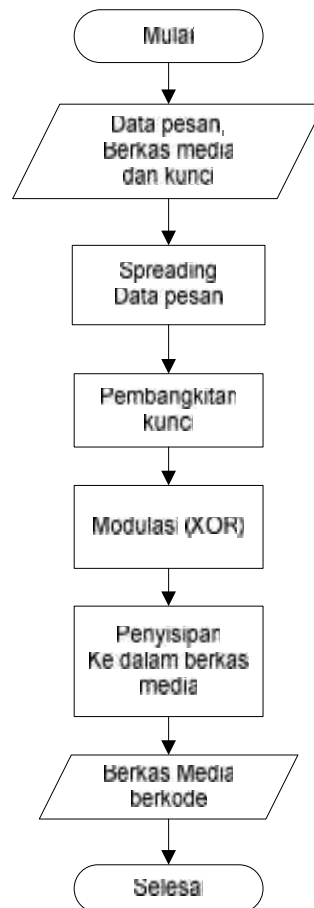
Dalam membangun aplikasi Stegambar ini memiliki 3 komponen utama, yaitu subsistem pengelolaan data, subsistem pengelolaan modul dan subsistem pengelolaan dialog (*interface*).

#### **4.3.1. Perancangan *Flowchart***

Perancangan *flowchart* pada Aplikasi Stegambar terbagi dua yaitu *flowchart* penyisipan dan *flowchart* ekstraksi adalah sebagai berikut:

#### 4.3.1.1. *Flowchart* Penyisipan

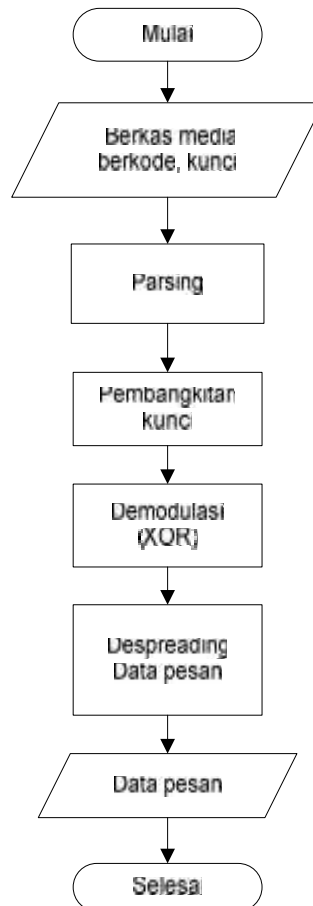
*Flowchart* penyisipan merupakan suatu cara menggambarkan algoritma dalam penyisipan data kedalam media.



Gambar 4.1 *Flowchart* Penyisipan

#### 4.3.1.2. Flowchart Ekstraksi

*Flowchart* ekstraksi merupakan suatu cara menggambarkan algoritma ekstraksi data sehingga diperoleh data pesan yang telah disisipkan.



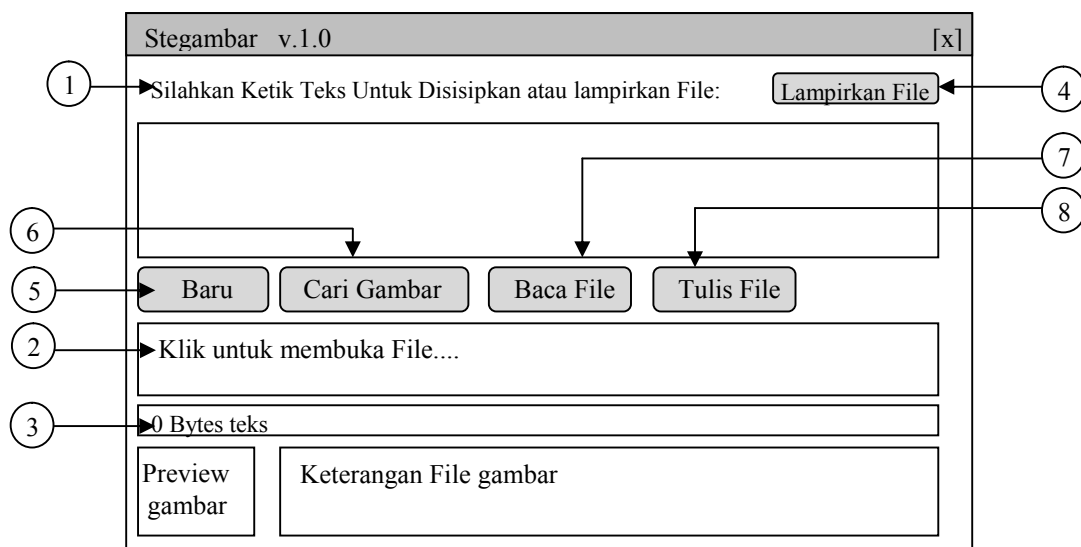
Gambar 4.2 *Flowchart* Ekstraksi

#### 4.3.2 PerancanganAntarmuka Sistem

Agar aplikasi memiliki sifat *user friendly*, maka perlu dirancang tampilan-tampilan yang mudah dipahami pengguna, sehingga pengguna mudah menggunakan aplikasi ini. Berikut ini beberapa rancangan tampilan proses penyembunyian dan pengekstraksian pesan.

#### 4.3.2.1 Antarmuka Menu utama

Rancangan antarmuka menu utama yang merupakan antarmuka utama Stegambar dapat dilihat pada gambar 4.3. Pengguna dapat memasukkan pesan rahasia ataupun data dan berkas Citra digital yang dijadikan media pembawa. Pengguna juga dapat memasukkan kunci rahasia untuk menambah aspek keamanan pesan rahasianya. Nama berkas hasil proses penyembunyian serta lokasinya juga ditentukan oleh pengguna.



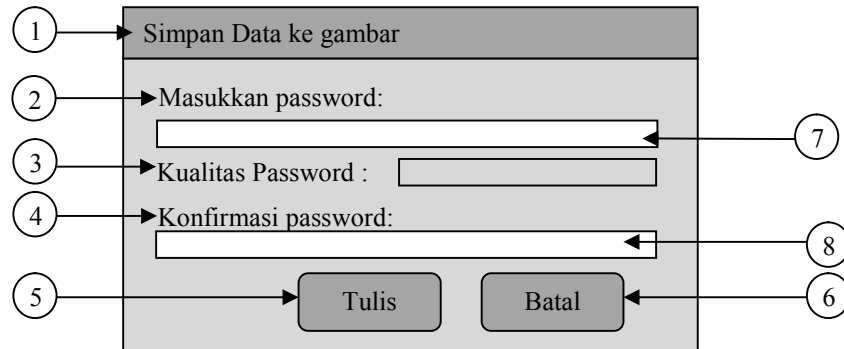
Gambar 4.3 Perancangan tampilan menu utama aplikasi Stegambar

Tabel 4.1 Tabel Keterangan Antarmuka menu utama aplikasi Stegambar

No	Objek	Properti	Pengaturan
1	Label 1	Caption	Silahkan Ketik Teks Untuk Disisipkan atau lampirkan File:
2	Label 2	Caption	Klik untuk membuka File....
3	Label 3	Caption	0 Bytes teks
4	Command Button 1	Caption	Lampirkan File
5	Command Button 2	Caption	Baru
6	Command Button 3	Caption	Cari Gambar
7	Command Button 4	Caption	Baca File
8	Command Button 5	Caption	Tulis File

#### 4.3.2.2 Antarmuka input *Password*

Rancangan antarmuka input password dapat dilihat pada gambar 4.9 dan 4.10. Pengguna memasukkan kunci rahasia (*password*) untuk menyimpan pesan rahasia ke dalam gambar dan pada saat pengguna membaca atau membuka data pesan dari gambar. Panjang karakter *password* minimal 5 karakter.

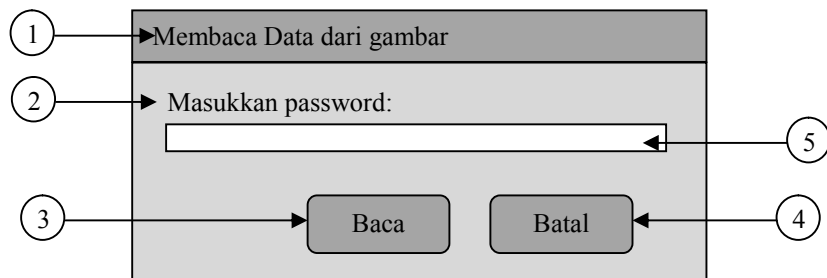


Gambar 4.4 Perancangan tampilan *input password* untuk menulis pesan pada gambar

Tabel 4.2 Tabel Keterangan Antarmuka input password untuk menulis pesan pada gambar

No	Objek	Properti	Pengaturan
1	Form	Caption	Simpan Data ke Gambar
2	Label 1	Caption	Masukkan Password :
3	Label 2	Caption	Kualitas Password
4	Label 3	Caption	Konfirmasi Password
5	Command Button 1	Caption	Tulis
6	Command Button 2	Caption	Batal
7	Text 1	Password char	*
8	Text 2	Password char	*





Gambar 4.5 Perancangan tampilan *input password* untuk membaca pesan

Tabel 4.3 Tabel Keterangan Antarmuka *input password* untuk membaca pesan pada berkas citra digital

No	Objek	Properti	Pengaturan
1	Form	Caption	Membaca Data dari Gambar
2	Label 1	Caption	Masukkan Password :
3	Command Button 1	Caption	Baca
4	Command Button 2	Caption	Batal
5	Text 1	Password char	*

## **BAB V**

### **IMPLEMENTASI DAN PENGUJIAN**

#### **5.1 Implementasi**

Implementasi merupakan lanjutan dari tahap perancangan yaitu aplikasi siap dioperasikan pada keadaan yang sebenarnya, sehingga akan diketahui apakah aplikasi yang dibuat telah menghasilkan tujuan yang diinginkan. Pada bagian ini diberikan gambaran mengenai implementasi perangkat lunak Stegambar berdasarkan hasil perancangan yang telah dibuat pada Bab sebelumnya. Pada Bab ini meliputi batasan implementasi, lingkungan implementasi, serta implementasi antarmuka hasil perancangan.

##### **5.1.1 Batasan Implementasi**

Batasan untuk implementasi perangkat lunak Stegambar adalah sebagai berikut:

- a. Berkas citra digital yang dimasukkan sebagai media pembawa data pesan hanya berkas citra digital dengan format *\*.BMP*
- b. Keluaran atau *output file* gambar yang telah disisipi pesan disimpan dengan format *\*.BMP*.

##### **5.1.2 Lingkungan Implementasi**

Lingkungan implementasi sistem ada dua yaitu lingkungan perangkat keras dan lingkungan perangkat lunak.

###### **5.1.2.1 Lingkungan Perangkat Keras**

Perangkat keras yang digunakan mempunyai spesifikasi sebagai berikut:

1. *Processor* Pentium IV 2.4 GHz
2. Memori RAM minimal 512 MB
3. *Hard Disk* minimal 80 GB
4. Monitor
5. *Keyboard* dan *Mouse*

### 5.1.2.2 Lingkungan Perangkat Lunak

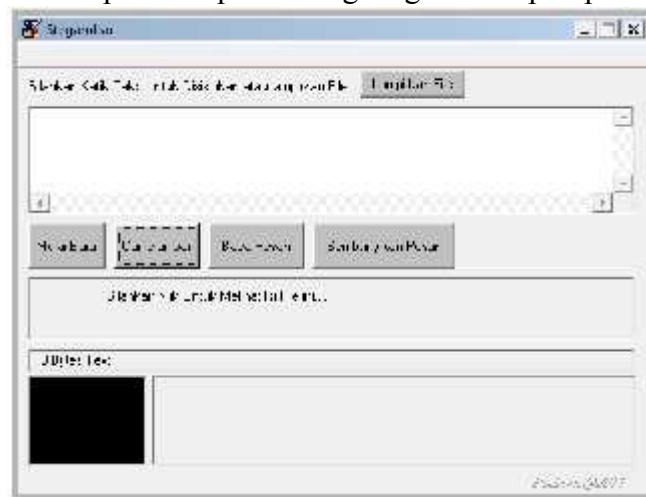
Perangkat lunak Stegambar dikembangkan pada komputer dengan sistem operasi *Microsoft Windows Xp Professional Service Pack 2*. Aplikasi yang digunakan dalam Implementasi perangkat lunak Stegambar adalah *Microsoft Visual Basic*.

## 5.2 Pengujian

Pengujian dilakukan dengan memperlihatkan penyisipan data teks dan karakter ke dalam berkas citra digital serta penyisipan file dokumen ke dalam berkas citra digital. Kemudian pembuktian dilakukan untuk membuktikan bahwa teks dan file yang dihasilkan setelah ekstraksi adalah sesuai dengan masukan (*input*). Pengujian meliputi pengujian aplikasi (tampilan aplikasi dan navigasi aplikasi) dan pengujian stegano analisis.

### 5.2.1 Pengujian Tampilan Aplikasi Stegambar

Pengujian dilakukan dengan melihat tampilan masing-masing tampilan yang ada dalam setiap urutan proses steganografi maupun pada proses ekstraksi.

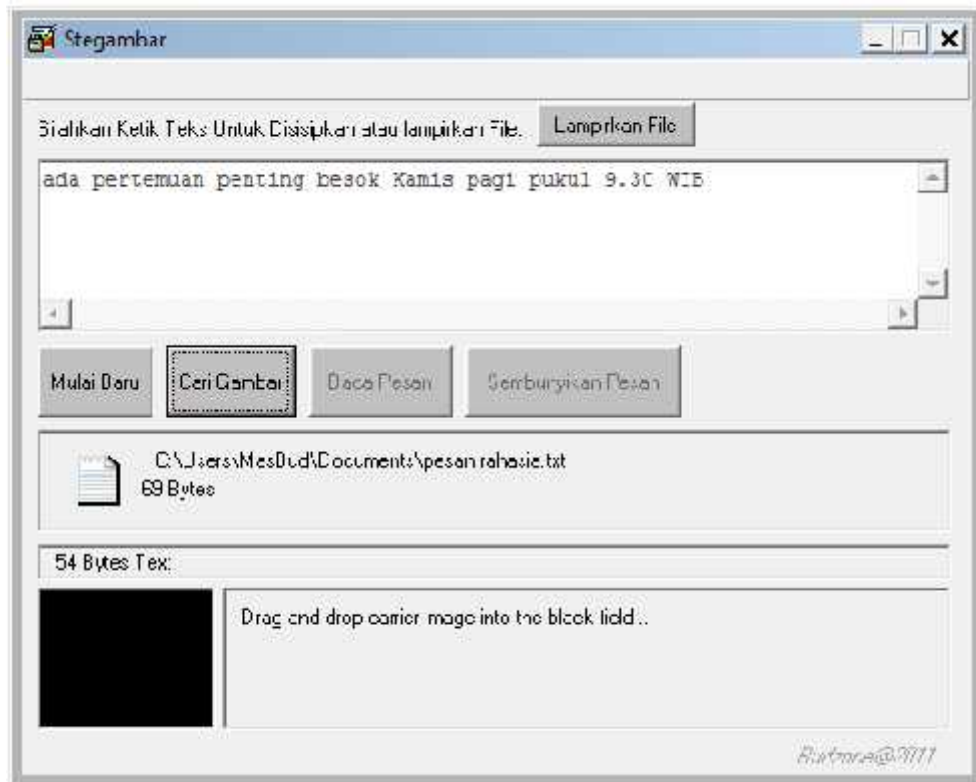


Gambar 5.1 Tampilan Menu Utama Aplikasi Stegambar

- a. Tampilan proses penyisipan teks kedalam berkas citra digital.

Pada tampilan awal diperlihatkan *menu* utama yang berfungsi untuk menentukan proses yang dilakukan yaitu proses penyisipan dan proses

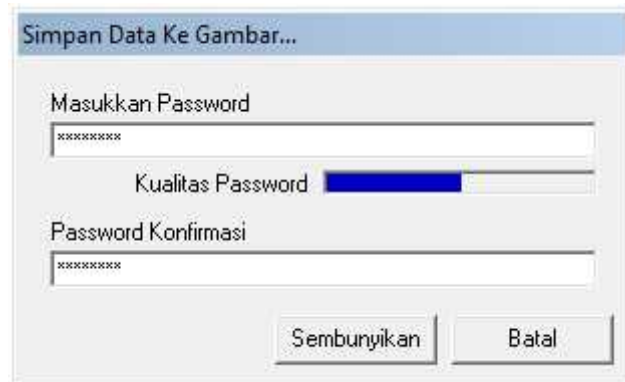
ekstraksi. Untuk menyembunyikan pesan, pengguna dapat memasukkan data yang akan diinputkan berupa teks pesan. Pengguna dapat juga melampirkan file dokumen dengan menekan tombol **Lampirkan File**.



Gambar 5.2 Tampilan Aplikasi Stegambar proses *input* data pesan

Selanjutnya Pengguna diminta memasukkan berkas citra digital sebagai media penyembunyian data dengan menekan tombol **Cari Gambar**. Berkas gambar yang dimasukkan adalah berkas citra digital dengan format *BMP*. *Output* berkas citra digital yang telah disisipi pesan adalah berkas citra digital dengan format *BMP*. Setelah data pesan dan data berkas gambar telah terisi, maka pengguna dapat menekan tombol **Sembunyikan Pesan**.

Tahap selanjutnya Pengguna diminta untuk memasukkan kata kunci atau Password. Setiap karakter Kata kunci yang dimasukkan tidak akan ditampilkan, tetapi ditampilkan dalam bentuk karakter bintang asteriks (\*). Setelah memasukkan kata kunci atau *Password*, Pengguna dapat menekan tombol **Sembunyikan**.



Gambar 5.3 Tampilan proses *input Password* untuk penyisipan pesan

b. Pengujian tampilan proses ekstraksi hasil.

Pada tampilan awal diperlihatkan menu utama yang berfungsi untuk menentukan proses yang dilakukan baik proses penyisipan maupun ekstraksi. Untuk melakukan ekstraksi data pesan, terlebih dahulu pengguna menentukan berkas citra digital yang telah disisipi data pesan dengan menekan tombol **Cari Gambar**. Selanjutnya pengguna dapat meng-ekstraksi pesan dengan menekan tombol **Baca Pesan**. Pengguna diminta untuk memasukkan kata kunci atau *password* sesuai dengan kata kunci pada saat data pesan disisipkan.



Gambar 5.4 Tampilan proses *input password* untuk ekstraksi

- c. Pengujian Tampilan Pesan kesalahan memasukkan *password*

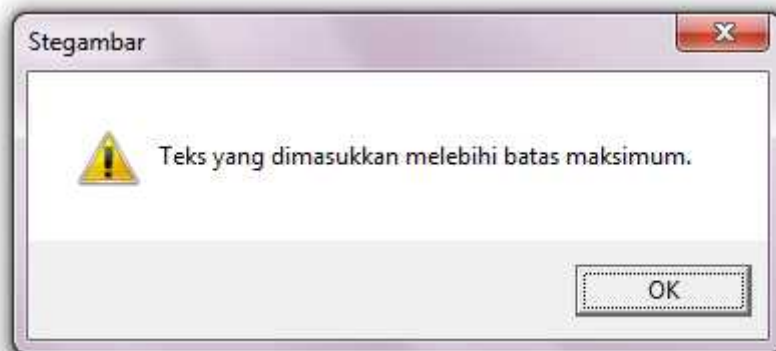
Pesan dibawah ini muncul apabila pengguna memasukkan *password* konfirmasi yang berbeda dengan sebelumnya pada saat akan menyisipkan data pesan.



Gambar 5.5 Tampilan pesan kesalahan memasukkan *password* konfirmasi

- d. Pengujian Tampilan Pesan Melebihi Batas Maksimum

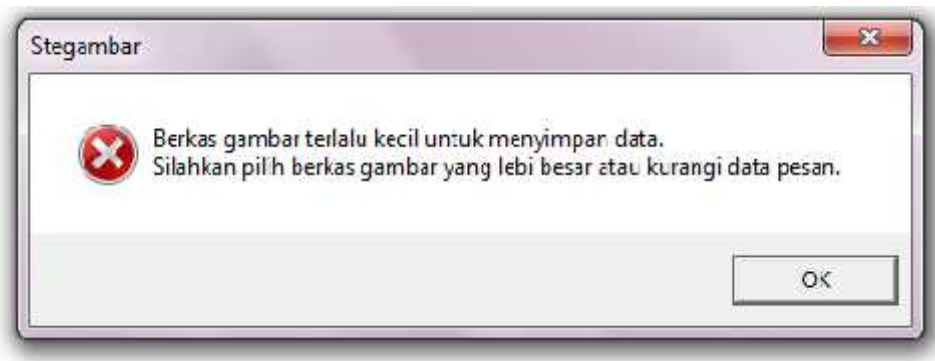
Apabila pengguna memasukkan teks pesan yang melebihi batas maksimum, maka aplikasi akan memberikan pesan seperti dibawah ini:



Gambar 5.6 Tampilan pesan melebihi batas maksimum

- e. Pengujian Tampilan Pesan ukuran berkas gambar kurang besar

Apabila ukuran berkas citra digital tidak mencukupi untuk menampung data pesan, maka aplikasi akan memberikan pesan sebagai berikut:



Gambar 5.7 Tampilan pesan ukuran berkas gambar kurang besar

### 5.3. Deskripsi Pengujian

Model atau cara pengujian pada aplikasi Stegambar Menggunakan metode *Black Box*.

#### 5.3.1 Pengujian Modul Menyembunyikan Teks Dalam berkas citra digital.

Pengujian modul ini merupakan hasil pengujian implementasi aplikasi secara detail mengenai item-item yang terdapat pada setiap tampilan proses menyembunyikan teks dalam berkas citra digital.

### 5.3.1.1 Pengujian Tahap I Mencari sumber Citra digital dan Lokasi penyimpanan

Prekondisi: Sudah ada sumber berkas citra digital didalam perangkat penyimpanan yang akan dilakukan pengujian

Tabel 5.1 Butir Uji Pengujian Tahap 1 Mencari Sumber Citra Digital Dan Lokasi Penyimpanan

Deskripsi	Prekondisi	Prosedur Pengujian	Masukan	Keluaran yang diharapkan	Kriteria Evaluasi Hasil	Hasil yang didapat	Kesimpulan
Pengujian tahap 1 mencari sumber citra digital dan lokasi penyimpanan	Tampilan layar menu utama,	<ol style="list-style-type: none"> <li>1. pada tampilan menu utama, tekan tombol "Cari Gambar"</li> <li>2. cari gambar yang akan diuji</li> <li>3. Tekan tombol "Open"</li> <li>4. Jika gambar yang dipilih bukan gambar berformat BMP, muncul pemberitahuan bahwa gambar akan dikonversi ke format BMP, tekan tombol "Yes"</li> </ol>	Berkas citra digital format BMP, JPG atau GIF	Proses pembacaan berkas citra digital berhasil, tidak ada instruksi error	Proses pembacaan berkas citra digital berhasil, tidak ada instruksi error	Proses pembacaan berkas citra digital berhasil, tidak ada instruksi error	Di terima



### 5.3.1.2 Pengujian Tahap 2 Memasukkan Data Pesan Yang Akan Disembunyikan

Prekondisi : Tahap 1 telah dilalui tidak ada instruksi error

Tabel 5.2 Butir Uji Pengujian Tahap 2 Memasukkan Data Pesan Yang Akan Disembunyikan

Deskripsi	Prekondisi	Prosedur Pengujian	Masukan	Keluaran yang diharapkan	Kriteria Evaluasi Hasil	Hasil yang didapat	Kesimpulan
Pengujian Tahap 2 memasukkan data pesan yang akan disembunyi kan	Tampilan layar menu utama, Tahap 1 telah dilalui tidak ada instruksi error	<ol style="list-style-type: none"> <li>1. Pada <i>textbox</i> tampilan menu utama, masukkan teks yang akan disembunyikan</li> <li>2. Apabila akan melampirkan file, tekan tombol “Lampirkan”</li> <li>3. Cari berkas data yang akan dilampirkan.</li> <li>4. Tekan tombol “Open”</li> </ol>	Pesan teks yang akan dimasukan, Data dokumen yang akan dilampirkan	Data pesan teks berhasil ditulis, Data dokumen berhasil dilampirkan, tidak ada instruksi error	Data pesan teks berhasil ditulis, Data dokumen berhasil dilampirkan, tidak ada instruksi error	Data pesan teks berhasil ditulis, Data dokumen berhasil dilampirkan, tidak ada instruksi error	Di terima

### 5.3.1.3 Pengujian Tahap 3 Proses Steganografi dan Memasukkan Kata Kunci

Prekondisi : Tahap 1 dan 2 telah dilalui tidak ada instruksi error

Tabel 5.3 Butir Uji Pengujian Tahap 3 Proses Steganografi dan Memasukkan Kata Kunci

Deskripsi	Prekondisi	Prosedur Pengujian	Masukan	Keluaran yang diharapkan	Kriteria Evaluasi Hasil	Hasil yang didapat	Kesimpulan
Pengujian Tahap 3 Proses Steganografi dan Memasukkan Kata Kunci	Tampilan layar menu utama, Tahap 1 dan 2 telah dilalui, tidak ada instruksi error	<ol style="list-style-type: none"> <li>1. Pada tampilan menu utama, tekan tombol “Sembunyikan Pesan”</li> <li>2. Masukkan kata kunci beserta konfirmasinya</li> <li>3. Tekan tombol “Sembunyikan”</li> </ol>	Kata kunci beserta konfirmasinya	Kata kunci berhasil dimasukkan, Data pesan teks berhasil disembunyikan, Data dokumen berhasil dilampirkan, tidak ada instruksi error	Kata kunci berhasil dimasukkan, Data pesan teks berhasil disembunyikan, Data dokumen berhasil dilampirkan, tidak ada instruksi error	Kata kunci berhasil dimasukkan, Data pesan teks berhasil disembunyikan, Data dokumen berhasil dilampirkan, tidak ada instruksi error	Di terima

### 5.3.2 Pengujian Modul Mengambil Data Pesan Dalam Berkas Citra Digital

Pengujian modul ini merupakan hasil pengujian implementasi aplikasi secara detail mengenai item-item yang terdapat pada setiap tampilan proses mengambil pesan teks dalam berkas citra digital.

#### 5.3.2.1 Pengujian Tahap 1 Menentukan Berkas Citra Digital Hasil Stegano Yang Akan Diambil Data Pesannya

Prekondisi : Sudah ada sumber file citra digital hasil stegano didalam perangkat penyimpanan yang akan dilakukan pengujian

Tabel 5.4 Butir Uji Pengujian Tahap 1 Menentukan Berkas Citra Digital Hasil Stegano Yang Akan Diambil Data Pesannya

Deskripsi	Prekondisi	Prosedur Pengujian	Masukan	Keluaran yang diharapkan	Kriteria Evaluasi Hasil	Hasil yang didapat	Kesimpulan
Pengujian Tahap 1 menentukan berkas citra digital hasil stegano yang akan diambil data pesannya	Tampilan layar menu utama	1. pada tampilan menu utama, tekan tombol "Cari Gambar" 2. cari berkas citra digital hasil stegano yang akan diuji 3. Tekan tombol "Open"	Berkas citra digital format BMP	Proses pembacaan berkas citra digital berhasil, tidak ada instruksi error	Proses pembacaan berkas citra digital berhasil, tidak ada instruksi error	Proses pembacaan berkas citra digital berhasil, tidak ada instruksi error	Di terima

### 5.3.2.2 Pengujian Tahap 2 Memasukkan Kata Kunci

Prekondisi : Tahap 1 telah dilalui tidak ada instruksi error

Tabel 5.5 Butir Uji Pengujian Tahap 2 Memasukkan Kata Kunci

Deskripsi	Prekondisi	Prosedur Pengujian	Masukan	Keluaran yang diharapkan	Kriteria Evaluasi Hasil	Hasil yang didapat	Kesimpulan
Pengujian Tahap 2 Memasukkan Kata Kunci	Tampilan layar menu utama, Tahap 1 telah dilalui, tidak ada instruksi error	<ol style="list-style-type: none"> <li>1. Pada tampilan menu utama, tekan tombol “baca Pesan”</li> <li>2. Setelah tampil form untuk memasukkan kata kunci, Silahkan ketik kata kucinya</li> <li>3. Tekan tombol ”Baca”</li> </ol>	Kata kunci	Jika kata kunci benar masuk keproses berikutnya jika salah tampil pesan kesalahan dan tidak ada instruksi error.	Jika kata kunci benar masuk keproses berikutnya jika salah tampil pesan kesalahan dan tidak ada instruksi error.	Jika kata kunci benar masuk keproses berikutnya jika salah tampil pesan kesalahan dan tidak ada instruksi error.	Di terima

### 5.3.2.3 Pengujian Tahap 3 Mengambil Data Pesan Teks Dalam Berkas Citra Digital

Prekondisi : Tahap 1 dan 2 telah dilalui tidak ada instruksi error

Tabel 5.6 Butir Uji Pengujian Tahap 3 Mengambil Pesan Teks Dalam citra digital

Deskripsi	Prekondisi	Prosedur Pengujian	Masukan	Keluaran yang diharapkan	Kriteria Evaluasi Hasil	Hasil yang didapat	Kesimpulan
Pengujian Tahap 3 mengambil data pesan teks dalam berkas citra digital	Tampilan layar menu utama, Tahap 1 dan 2 telah dilalui, tidak ada instruksi error	<ol style="list-style-type: none"> <li>Setelah memasukkan kata kunci dan menekan tombol “Baca”, Pesan teks akan tampil pada <i>textbox</i> Pada tampilan menu utama,</li> <li>Apabila ada data lampiran yang terbaca, muncul pesan apakah akan disimpan pada folder yang sama?</li> <li>Tekan tombol “Yes” untuk menyimpan data Lampiran</li> </ol>	-	Proses pengambilan data pesan berhasil, tampil informasi pesan teksnya dan tidak ada instruksi error	Proses pengambilan data pesan berhasil, tampil informasi pesan teksnya dan tidak ada instruksi error	Proses pengambilan data pesan berhasil, tampil informasi pesan teksnya dan tidak ada instruksi error	Di terima

#### 5.4. Pengujian Berdasarkan Kriteria Steganografi

Setelah dilakukan pengujian terhadap aplikasi Stegambar, didapatkan hasil sebagai berikut:

##### 5.4.1 Pengujian Berdasarkan *Imperceptibility*

Pengujian *Imperceptibility* yaitu menguji kualitas berkas media pembawa data pesan apakah media pembawa mengalami perubahan yang mencurigakan atau tidak. Pengujian ini dikatakan berhasil apabila kualitas berkas yang dihasilkan tidak mengalami distorsi yang besar dibandingkan dengan berkas aslinya. Citra digital dari berkas yang dihasilkan tidak jauh berbeda dari berkas aslinya.



Gambar 5.9. Berkas citra digital cat.bmp asli



Gambar 5.10. Berkas citra digital cat.bmp setelah disisipkan data pesan

#### 5.4.2 Pengujian Berdasarkan *Fidelity*

Proses penyembunyian data dapat berhasil apabila ukuran data yang akan disembunyikan lebih kecil atau sama dengan kapasitas data yang dapat ditampung. Apabila ukuran data lebih besar dan kapasitas data yang dapat ditampung, maka aplikasi tidak akan melanjutkan proses penyembunyian. Kapasitas data dipengaruhi oleh ukuran berkas citra digital. Semakin besar ukuran berkas citra digital, maka semakin besar pula kapasitas yang akan dihasilkan.

Tabel 5.7 Tabel Hasil pengujian penyembunyian data.

Berkas Citra ( <i>Stego image</i> )	Ukuran	Kapasitas Pesan	Lampiran		Hasil
			Berkas	Ukuran	
cat.bmp	88 Kb	43 Bytes	-	-	Berhasil
desert.bmp	2.304 Kb	228 KB	Tugas SKI.docx	228 KB	Berhasil
koala.bmp	791 Kb	-	Kunci jawaban.doc	13.7 KB	Berhasil
Mekah.bmp	766 Kb	-	Kunci jawaban.doc	13.7 KB	Berhasil
Penguins.bmp	352 Kb	-	Pesan.txt	94 Bytes	Berhasil

#### 5.4.3 Pengujian Berdasarkan *Recovery*

Untuk menentukan apakah perangkat lunak ini telah memenuhi spesifikasi, maka harus dapat dibuktikan bahwa berkas citra digital dapat diekstraksi. Agar data dapat diekstraksi, maka syaratnya adalah kunci yang digunakan harus sesuai dengan kunci yang digunakan saat proses penyembunyian data.

Jika pengujian dilakukan dengan benar maka data rahasia dapat ditampilkan (diekstrak) sesuai dengan data yang dimasukkan. Sedangkan jika pengujian menggunakan masukan kunci yang salah, maka tidak memberikan data yang sesuai dengan harapan.

Kegagalan ekstraksi data pada penelitian ini terjadi karena kunci yang salah. Data yang dihasilkan dari proses ekstraksi tidak ada sama sekali, atau menghasilkan karakter-karakter aneh yang tidak dapat dibaca. Hasil dari pengujian ekstraksi pesan dapat dilihat pada tabel 5.8

Tabel 5.8 Tabel Hasil pengujian Ekstraksi data Pesan.

Berkas Citra ( <i>Stego image</i> )	Ukuran	Kapasitas Pesan	Lampiran		Hasil
			Berkas	Ukuran	
cat.bmp	88 Kb	43 Bytes	-	-	Berhasil
desert.bmp	2.304 Kb	228 KB	Tugas SKI.docx	228 KB	Berhasil
koala.bmp	791 Kb	-	Kunci jawaban.doc	13.7 KB	Berhasil
Mekah.bmp	766 Kb	-	Kunci jawaban.doc	13.7 KB	Berhasil
Penguins.bmp	352 Kb	-	Pesan.txt	94 Bytes	Berhasil

#### 5.4.4 Pengujian Kesesuaian Data

Pengujian kesesuaian data yaitu pengujian dengan cara membandingkan ukuran file antara berkas yang telah disisipkan pesan dengan berkas yang masih asli. Pengujian ini dimaksudkan untuk mengetahui apakah ukuran berkas yang telah disisipkan data sama dengan berkas yang asli, yaitu dilakukan dengan cara membandingkan secara langsung dan dengan menggunakan kompresi.

Pengujian dapat dilakukan dengan membandingkan ukuran berkas asli dengan berkas yang telah disisipkan data rahasia. Pengujian kapasitas *file* dilakukan dalam 5 kali pengujian. Hasil pengujian dapat dilihat pada tabel berikut:

Tabel 5.9 Perbandingan ukuran berkas asli dengan berkas hasil steganografi.

No	Berkas Citra Digital Asli		Berkas hasil Steganografi	
	Nama File	Ukuran	Nama File	Ukuran
1	Cat asli.bmp	88 Kb	cat.bmp	88 Kb
2	Desert asli.bmp	2.304 Kb	Desert.bmp	2.304 Kb
3	Koala asli.bmp	791 Kb	Koala.bmp	791 Kb
4	Mekah asli.bmp	766 Kb	mekah.bmp	766 Kb
5	Penguins asli.bmp	352 Kb	Penguins.bmp	352 Kb



#### 5.4.5 Pengujian Berdasarkan *Robustness*

Pengujian dilakukan dengan melihat ketahanan data yang disembunyikan dalam berkas citra digital terhadap proses *editing* yang dilakukan pada berkas citra digital.

##### 5.4.5.1 Pengujian Proses *Editing* 1: *Cropping*

Pengujian dilakukan dengan memotong (*cropping*) sebagian berkas citra digital yang telah disisipkan pesan. Pada Gambar 5.11 memperlihatkan citra digital hasil steganografi yang berukuran 200x150 piksel telah dilakukan pemotongan (*cropping*) sebesar 60 piksel pada bagian kanan. Setelah dilakukan proses *cropping* mengakibatkan data pesan yang telah disisipkan didalamnya tidak dapat diungkap kembali.



Gambar 5.11 Berkas citra digital setelah dilakukan *cropping*

Pengujian dilakukan dalam 5 kali pengujian, adapun hasil pengujian dapat dilihat pada tabel berikut:

Tabel 5.10 Pengujian Pemotongan (*Cropping*)

No	File	Ukuran (Piksel)	Bagian Pemotongan	Ukuran (piksel)	Hasil
1	cat.bmp	200x150	Kanan	60	Ekstraksi Gagal
2	Desert.bmp	1024x768	Atas	156	Ekstraksi Gagal
3	Koala.bmp	600x450	Atas dan Bawah	50 + 50	Ekstraksi Gagal
4	mekah.bmp	639x409	Bawah	92	Ekstraksi Gagal
5	Penguins.bmp	400x300	Kiri dan kanan	60 + 60	Ekstraksi Gagal

Dari hasil pengujian diketahui bahwa proses pemotongan dapat merusak karakter teks yang berada dalam berkas citra digital, karena terjadinya perubahan letak biner. Hal ini terbukti dari proses ekstraksi hasil yang gagal dilakukan karena data pesan telah rusak. Pengujian membuktikan salah satu kelemahan penggunaan metode LSB.

#### 5.4.5.2 Pengujian Proses *Editing 2: Rotate*

Pengujian dilakukan dengan Memutar (*Rotate*) berkas citra digital yang telah disisipi pesan. Pada Gambar 5.12 memperlihatkan citra digital hasil steganografi yang berukuran 200x150 piksel telah dilakukan rotasi sebesar 180°. Setelah dilakukan proses rotasi mengakibatkan data pesan yang telah disisipkan didalamnya tidak dapat diungkap kembali.



Gambar 5.12 Berkas citra digital setelah dilakukan rotasi 180°

Pengujian dilakukan dalam 5 kali pengujian. Hasil pengujian dapat dilihat pada tabel berikut:

Tabel 5.11 Pengujian Pemutaran (*Rotate*)

No	File	Arah putaran	Hasil
1	cat.bmp	180°	Ekstraksi Gagal
2	Desert.bmp	90° CW	Ekstraksi Gagal
3	Koala.bmp	90° CCW	Ekstraksi Gagal
4	mekah.bmp	180°	Ekstraksi Gagal
5	Penguins.bmp	90° CW	Ekstraksi Gagal

Dari hasil pengujian diketahui bahwa proses pemutaran (*Rotate*) Pada berkas citra digital yang telah disisipi pesan dapat merusak karakter teks yang berada dalam berkas citra digital. Hal ini terbukti dari proses ekstraksi hasil yang gagal dilakukan karena data pesan telah rusak.

#### 5.4.5.3 Pengujian Proses *Editing 3: Resize*

Pengujian dilakukan dengan Merubah ukuran (*Resize*) berkas citra digital yang telah disisipi pesan. Pada Gambar 5.13 memperlihatkan citra digital hasil steganografi yang berukuran 200x150 piksel. Sedangkan Gambar 5.14 memperlihatkan citra digital yang telah dirubah ukurannya menjadi 300x225 piksel. Setelah dilakukan proses *resize* mengakibatkan data pesan yang telah disisipkan didalamnya tidak dapat diungkap kembali.



Gambar 5.13 Berkas citra digital sebelum dirubah ukurannya



Gambar 5.14 Berkas citra digital setelah dirubah ukurannya

Pengujian dilakukan dalam 5 kali pengujian. Hasil pengujian dapat dilihat pada tabel berikut:

Tabel 5.12 Pengujian Perubahan Ukuran (*Resize*)

No	File	Ukuran ( <i>Piksel</i> )		Perubahan Ukuran	Hasil
		Sebelum	Sesudah		
1	cat.bmp	200x150	300x225	+ 50%	Ekstraksi Gagal
2	Desert.bmp	1024x768	819x614	- 20%	Ekstraksi Gagal
3	Koala.bmp	600x450	300x225	- 50 %	Ekstraksi Gagal
4	mekah.bmp	639x409	575x368	- 10 %	Ekstraksi Gagal
5	Penguins.bmp	400x300	500x375	+ 25 %	Ekstraksi Gagal

Dari hasil pengujian diketahui bahwa proses Perubahan ukuran (*Resize*) Pada berkas citra digital yang telah disisipi pesan dapat merusak karakter teks yang berada dalam berkas citra digital. Hal ini terbukti dari proses ekstraksi hasil yang gagal dilakukan karena data pesan telah rusak.

## 5.5 Kesimpulan Pengujian

Setelah membandingkan antara hasil perancangan dan hasil yang didapat, maka dapat disimpulkan bahwa steganografi teks ke dalam berkas citra digital menggunakan metode *spread spectrum* dalam pengacakan pesan dan metode *least significant bit modification (LSB modification)* dalam menyisipkan pesan, dapat dilakukan dan dapat disimpulkan dari beberapa pengujian sebagai berikut:

1. Kapasitas file citra digital sebelum dan sesudah disisipkan data pesan tidak mengalami perubahan yang berarti.
2. Pengujian dilakukan dengan membandingkan berkas citra digital sebelum dilakukan steganografi dan berkas citra digital hasil steganografi. Dari hasil pengujian diperoleh hasil bahwa kualitas berkas citra digital tidak mengalami perubahan yang berarti.
3. Pengujian dilakukan dengan melihat data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung. Dari hasil pengujian diketahui bahwa proses editing pada citra digital hasil

steganografi seperti pemotongan (*crop*), Pemutaran (*Rotate*) dan Perubahan ukuran (*Resize*) dapat merusak data pesan yang berada dalam berkas citra digital, karena terjadinya perubahan letak biner. Hal ini terbukti dari proses ekstraksi hasil yang gagal dilakukan karena berkas citra digital yang telah rusak.

4. Pengujian dilakukan dengan menjalankan aplikasi ekstraksi hasil, dapat diambil kesimpulan bahwa pengungkapan data kembali berhasil dan aplikasi memenuhi syarat *recovery*.

## **BAB VI**

### **PENUTUP**

#### **6.1 Kesimpulan**

Berdasarkan analisa, perancangan dan implementasi pada aplikasi keamanan data menggunakan teknik steganografi pada citra digital dengan metode *spread spectrum* dalam pengacakan pesan dan metode *least significant bit (LSB) modification* dalam penyisipan pesan, dapat diambil kesimpulan sebagai berikut:

1. Steganografi pada citra digital dengan menerapkan metode *spread spectrum* dan *least significant bit modification* dapat melakukan penyembunyian data teks kedalam berkas gambar.
2. Steganografi dapat digunakan untuk proses penyembunyian suatu data pesan teks dalam berkas citra digital.
3. Metode *least significant bit (LSB)* dapat digunakan untuk menyisipkan data teks dan karakter ke dalam berkas citra digital.

#### **6.2 Saran**

Beberapa hal yang disarankan dalam pengembangan aplikasi steganografi pada citra digital dengan menerapkan metode *Spread spectrum* dan *LSB Modification* ini adalah sebagai berikut:

1. Pada aplikasi ini menggunakan berkas citra digital dengan format .BMP sebagai *file* penampung dan tidak menutup kemungkinan dikembangkan menggunakan berkas citra digital dengan format lain.
2. Dalam penyisipan data, aplikasi ini menggunakan metode *LSB*, dan disarankan untuk mengembangkannya dengan metode lain seperti metode *Masking and Filtering*, *Transformation* untuk membandingkan metode yang tepat untuk steganografi.

## DAFTAR PUSTAKA

- Adli, Dziky, *Tugas Akhir Audio Steganografi pada Bekas WAV dengan Metode Spread Spectrum*, Pekanbaru: UIN SUSKA Riau, 2008
- Ariyus, Dony, *Pengantar Ilmu Kriptografi (Teori Analisis dan Implementasi)*, Jogjakarta: Andi Offset, 2008
- Habibie, Dolie, *Tugas Akhir Steganografi pada video digital dengan menggunakan metode least significant bit modification*, Pekanbaru: UIN SUSKA Riau, 2008
- Masaleno, Andino, *Jurnal Pengantar Steganografi*,  
<http://fairuzelsaid.files.wordpress.com/2010/03/andino-steganografi.pdf>  
(diakses 12 Maret 2011)
- Muchtar, Nur Ali, *Paper Tugas Akhir Mata Kuliah: Kajian Tentang Steganografi*,  
<http://alymereunung.wordpress.com/2009/12/22/paper-tentang-steganografi/>, (diakses 12 Maret 2011)
- Munir, Rinaldi, *Pengolahan Citra Digital Dengan Pendekatan Algoritmik*, Bandung: Informatika, 2004
- Novrina, Indah Kusuma, *Jurnal Peningkatan Pengamanan Pesan Rahasia dengan Teknik Penyisipan Pada Citra Digital Menggunakan Pendekatan LSB*, Jakarta: Univ.Gunadarma, 2008
- Putra, Darma, *Pengolahan Citra Digital*, Jogjakarta: Andi Offset, 2010
- Sulianta, Feri, *Teknik Menyembunyikan File*, Jakarta: Elex Media Komputindo, 2009